FINAL REPORT
ON
THE LAW OF INFORMATION TECHNOLOGY

Introductory

After the invention of computers and improvement in digital technology and communication systems dramatic changes have taken place in our lives. Business transactions are being made with the help of computers. Computers are being increasingly used by the business community and individuals to create, transmit and store information in the electronic form instead of traditional paper documents. Information stored in electronic form is easier, cheaper, much less time-consuming and less cumbersome than storage in paper documents. Information stored in electronic form is also easier to retrieve and speedier to communicate. In spite of all these advantages and although they are aware of these advantages people in our country are reluctant to conduct business or conclude transactions in electronic form due to lack of legal framework. At present, many legal provisions (such as the Evidence Act, 1872, the Penal Code, 1860. the Banker's Books Evidence Act, 1891, etc.) recognise paper based records and documents bearing signatures of parties and make them admissible in evidence in various disputes. Electronic commerce eliminates the need for such paper based transactions and as such, transactions in electronic form are often not recognised in courts thereby retarding the growth of electronic commerce. Many legal rules assume the existence of paper records and documents, signed records, original records, physical cash, cheques, face to face meetings, etc. As more and more activities to-day are carried out by electronic means, it becomes more and more important that evidence of these activities be available to demonstrate legal rights and

obligations that flow from them. As such, in order to facilitate electronic commerce, there is a need for a legal framework and also for legal changes. In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted Model Law on electronic commerce known as the UNCITRAL Model Law on Electronic Commerce hereinafter referred to as the Model Law.

The Model Law establishes rules and norms that validate and recognize contracts formed through electronic means, sets default rules for contract formation and governance of electronic contract performance, defines the characteristics of a valid electronic writing and an original document, provides for the acceptability of electronic signatures for legal and commercial purposes and supports the admission of computer evidence in courts and arbitration proceedings. The Model Law does not have any force but merely serves as a model to countries for the evaluation and modernization of certain aspects of their laws and practices in the field of communication involving the use of computerized or other modern techniques, and for the establishment of relevant legislation where none exists.

In the above context, it is proposed to suggest enactment of a suitable law to facilitate electronic commerce and to encourage growth and development of information technology. Necessarily, such law has to be in conformity with the Model Law.

Singapore enacted Electronic Transactions Act, 1998 and India recently enacted the Information Technology Act, 2000.

The objectives of the proposed legislation are to give effect to the following purposes:-

(a) to facilitate electronic communications by means of reliable electronic records;

(b) to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature

requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(c) to facilitate electronic filing of documents with government agencies and statutory corporations, and to promote efficient delivery of government services by means of reliable electronic records;

(d) to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;

(e) to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and

(f) to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

While preparing this report proposing enactment of a law on electronic commerce the following matters are, therefore, required to be addressed in order to achieve the above purposes:-

1) Applicability of the Act;

2) The "Functional Equivalent" approach;

3) Electronic documents and electronic contracts;

4) Electronic governance;

5) Electronic signatures;

6) The technology for electronic signatures;

7) Liability and risk allocation in a Public Key Infrastructure (PKI);

8) Procedural aspects of PKI;

9) Contraventions;

10) Cyber Regulations Appellate Tribunal (CRAT);

11) Information technology offences;

12) Investigation, search and seizure;

13) Limited liability of Network Services Providers;

14) Cyber Regulations Advisory Committee;

15) Amendment/ repeal, etc., of related enactments.

Article 1 of the Model Law defines the sphere of application of the law as follows:-

"This Law applies to any kind of information in the form of a data message used in the context of commercial activities."

While limiting the applicability of the law to data messages in the context of only "commercial activities", in the substantive part of the Model Law, the United Nations Commission on International Trade Law (UNCITRAL) hereinafter referred to as the Commission made various alternative suggestions such as, it suggested for the states which might wish to limit the applicability of the Act to only international data messages the following text:- "The Law applies to a data message where the data message relates to international commerce"; and for the states that might wish to extend the applicability of the law, the following text:- "This Law applies to any kind of information in the form of data message, except in the following situations:"

The Commission also suggested to give the word "commercial" occurring in Article 1 of the Model Law the widest possible interpretation in order to include every conceivable transaction of a commercial nature.[1]

On due consideration, it appears to us that the applicability of the Act need not be limited by using the term "commercial" as in Article 1 of the Model Law. The applicability should be wide enough and this purpose can be

[1] UNCITRAL, Model Law on Electronic Commerce, 1996, Article 1.

achieved by simply excluding certain matters specifically from its jurisdiction. In her Information Technology Act, 2000, India has excluded documents relating to the following five specific matters from the jurisdiction of the Act and has also authorized the Government to exclude any other documents: (1) negotiable instruments, (2) powers of attorney, (3) trusts, (4) wills, (5) contracts for the sale or conveyance of immovable property and (6) any other documents or transactions as the Government may notify and except the above, the Act applies to all circumstances, types of transactions and documents.[2] The Indian Act also extends the applicability relating to offences and contraventions beyond her territories.[3] It also overrides all other laws in force in India.[4]

In Singapore, the corresponding law is the Electronic Transactions Act, 1998. Following the second alternative suggestion made by the Commission in the Model Law, Singapore also sought to widen the applicability of the law by excluding the following transactions from the operation of the law:- (a) wills; (b) negotiable instruments; (c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts; (d) contract for the sale or other disposition of immovable property, or any interest in such property; (e) the conveyance of immovable property or the transfer of any interest in immovable property; (f) documents of title and also authorised the Government to add, delete or amend any class of transactions or matters.[5] It appears to us that in some respects the Indian provisions and in some respects the Singapore provisions regarding the applicability of the law are precise and clear. After taking into consideration the provisions and suggestions in the Model Law and the provisions of the Indian and the Singapore enactments we propose the short title, commencement, extent and applicability of the proposed Act as follows:-

[2] Information Technology Act, 2000 (India), section 1.
[3] Ibid, section 75.
[4] Ibid, section 81.
[5] (Singapore) Electronic Transactions Act, 1998, section 4.

Chapter I

PRELIMINARY

"1. Short title, extent and commencement.- (1) This Act may be called the Information Technology (Electronic Transaction) Act, 20----------.

(2) It shall extend to the whole of Bangladesh and, save as otherwise expressly provided in this Act, also to any offence or contravention thereunder committed outside Bangladesh by any person.

(3) It shall come into force on such date as the Government may, by notification in the Official Gazette, appoint.

"2. Application.- (1) Nothing in this Act shall apply to-

(a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881 (Act No. XXVI of 1881);

(b) the creation, performance or enforcement of a power of attorney;

(c) a trust as defined in section 3 of the Trusts Act, 1882 (Act No. II of 1882);

(d) a will as defined in clause (h) of section 2 of the Succession Act, 1925 (Act No. XXXIX of 1925) and any other testamentary disposition by whatever name called;

(e) any contract for the sale or other disposition of immovable property, or any interest in such property;

(f) the conveyance of immovable property or the transfer of any interest in immovable property; and

(g) title-deeds of immovable property;

(2) The Government may, by notification in the Official Gazette, modify the provisions of sub-section (1) of this section by adding, deleting or amending any class of transactions or matters."

Next comes interpretation of various terms and expressions to be used in the proposed Act. Some of these terms are technical in nature. Some of the terms used in the Indian enactment exactly correspond with similar terms used in the Singapore enactment. Some terms have been defined as proposed in the Model Law. After taking into considerations the interpretations in the Model Law, the Indian enactment and the Singapore enactment, we propose to suggest the interpretation of various terms as follows:-

"3. Definitions.- In this Act, unless the context otherwise requires,-

(a) "access" means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;

(b) "act" has the same meaning as in the Penal Code, 1860 (Act XLV of 1860);

(c) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(d) "adjudicating officer" means an adjudicating officer appointed under sub-section (1) of section 50 of this Act;

(e) "affixing digital signature" means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

(f) "asymmetric cryptosystem" means a system capable of generating a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) "Certifying Authority" means a person who has been granted a licence under section 25 of this Act to issue a Digital Signature Certificate;

(h) "certification practice statement" means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

(i) "computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetical and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;

(j) "computer network" means the interconnection of one or more computers through-

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) "computer resource" means computer, computer system, computer network, data, computer database or software;

(l) "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m) "Controller" means the Controller of Certifying Authorities appointed under sub-section (1) of section 18 of this Act;

(n) "Cyber Appellate Tribunal" means the Cyber Appellate Tribunal established under sub-section (1) of section 52 of this Act;

(o) "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been

prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(p) "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with section 4 of this Act;

(q) "Digital Signature Certificate" means a certificate issued under sub-section (1) of section 36 of this Act;

(r) "electronic form", with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated microfiche or similar device;

(s) "Electronic Gazette" means the Official Gazette published in the electronic form;

(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche;

(u) "function", in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(v) "hash function" means an algorithm mapping or translating one sequence of bits into another, generally smaller, set known as the "hash result" such that –

(i) an electronic record yields the same hash result every time the algorithm is executed using the same electronic record as input;

(ii) it is computationally infeasible that an electronic record can be derived or reconstituted from the hash result produced by the algorithm;

(iii) it is computationally infeasible that two electronic records can be found that produce the same hash result using the algorithm;

(w) "information" includes data, text, images, sound, voice, codes, computer programmes, software, databases, microfilm, or computer generated microfiche;

(x) "intermediary", with respect to any particular electronic message, means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

(y) "key pair", in an asymmetric cryptosystem, means a private key and its mathematically related public key, having the property that the public key can verify a digital signature created by the private key;

(z) "law" includes any Act of Parliament, Ordinances promulgated by the President and rules, regulations, bye-laws, notifications or other legal instruments having the force of law;

(za) "licence" means a licence granted to a Certifying Authority under section 25 of this Act;

(zb) "offence" denotes an act made punishable under any law for the time being in force in Bangladesh;

(zc) "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zd) "prescribed" means prescribed by rules made under this Act;

(ze) "private key" means the key of a key pair used to create a digital signature;

(zf) "public key" means the key of a key pair used to verify a digital signature and listed in a Digital Signature Certificate;

(zg) "secure system" means computer hardware, software, and procedure that –

(i) are reasonably secure from unauthorised access and misuse;

(ii) provide a reasonable level of reliability and correct operation;

(iii) are reasonably suited to performing the intended functions; and

(iv)adhere to generally accepted security procedures;

(zh) "security procedure" means a procedure prescribed by the Government under section 17 of this Act for the purpose of –

(i) verifying that an electronic record is that of a specific person; or

(ii) detecting error or alteration in the communication, content or storage of an electronic record since a specific point of time,

which may require the use of algorithms or codes, identifying words or numbers, encryption, answer back or acknowledgement procedures, or similar security devices;

(zi) "sign" has the same meaning as in clause (52) of section 3 of the General Clauses Act, 1897 (Act No. X of 1897) and also includes any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic or digital methods and the expression "signature" shall be construed accordingly;

(zj) "subscriber" means a person in whose name the Digital Signature Certificate is issued and who holds a private key that corresponds to a public key listed in that Digital Signature Certificate;

(zk) "verify", in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions, means to determine accurately whether –

(a) the initial electronic record was affixed with the digital signature by the use of the private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature".

In the next sections, provisions may be made for legal recognition of electronic records, digital signatures, authentication of electronic records, etc. In Singapore, firstly, provisions have been made for legal recognition of electronic records specifying that information shall not be denied legal recognition, legal effect, validity or enforceability solely on the ground that the information is in the form of an electronic record. The Singapore law further provides that if any law requires any information to be in writing, that requirement is fulfilled if it is in an electronic record.[6] India has made similar provisions.[7] Singapore derived the principles of the above provisions from the Model Law.[8] In this respect, Singapore has adopted the language of the Model Law to a large extent. India's formulation is somewhat different but the principles embodied are the same as in the Model Law. Similar provisions have been made regarding digital signatures in both Singapore law and the Indian law following the Model Law.[9] For incorporating the above principles we like to propose the following provisions:-

[6] (Singapore) Electronic Transactions Act, 1998, sections 6 and 7.
[7] (Indian) Information Technology Act, 2000, section 4.
[8] UNCITRAL Model Law, Articles 5, 5 bis and Article 6.
[9] Ibid, note (6), section 8; ibid, note (7), sections 3 and 5; and ibid, note (8) Article 7.

Chapter II

DIGITAL SIGNATURE & ELECTRONIC RECORDS

"4. Authentication of electronic records by digital signature.- (1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric cryptosystem and hash function which envelop and transform the initial electronic record into another electronic record.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

5. Legal recognition of electronic records.- Where any law requires any information or matter to be written, in writing or in the typewritten or printed form or provides for certain consequences if it is not, then notwithstanding such law, such requirement shall be deemed to have been met if such information or matter is rendered in an electronic form:

Provided that the information or matter is accessible so as to be usable for a subsequent reference.

6. Legal recognition of digital signatures.- Where any law requires that information or any matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person or provides for any consequences if it is not, then, notwithstanding any such law, such requirement shall be deemed to have been met, if such information or matter is authenticated or such document is signed by means of digital signature affixed in such manner as may be prescribed by the Government."

The next provision may provide for recognition and acceptance of electronic records and electronic signatures in various government offices, agencies, etc. because, in various existing laws there are mandatory provisions

for filing, recognition and acceptance of applications, forms, etc. in specified manner and also for issuance of licence, orders, permits, sanctions, etc. by governmental authorities in specified manner. The purpose of the proposed enactment will be largely frustrated if, notwithstanding the existing laws, enabling provision is not made regarding the electronic records and electronic signatures for their acceptance, recognition, etc. in government offices. We, accordingly, propose the following provision:-

"7. Use of electronic records and digital signatures in Government and its agencies.- (1) Where any law requires-

(a) the filing of any form, application or any other document with any office, body, authority or agency owned or controlled by the Government in a particular manner;

(b) the issue or grant of any licence, permit, sanction, approval or order by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner,

then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the Government.

(2) The Government may, for the purposes of sub-section (1) of this section, by rules, prescribe-

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue of any electronic record under clause (a) of this sub-section."

Under various laws and rules modes have been prescribed for retention and preservation of records and documents in various offices, courts, organisations, etc. and by individuals. Similarly, provisions are required to be

made for retention and preservation of electronic records as well. We, accordingly, propose the following provision:-

"8. Retention of electronic records.- (1) Where any law requires that any documents, records or information shall be retained for any specific period, then such requirement shall be deemed to have been satisfied if such documents, records or information, as the case may be, are retained in the electronic form if the following conditions are satisfied:-

(a) the information contained therein remains accessible so as to be usable for subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) such information, if any, as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained;

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(2) A person may satisfy the requirements referred to in sub-section (1) of this section by using the services of any other person, if the conditions in clauses (a) to (c) of that sub-section are complied with.

(3) Nothing in this section shall apply to any law which expressly provides for the retention of documents, records or information in the form of electronic records."

In clause (s) of section 3 of this Act we have defined "Electronic Gazette" attributing to it the same meaning as the "Official Gazette" as defined in clause (37 a) of section 3 of the General Clauses Act, 1897. In this Act, there must, therefore, be a provision giving the same status to all publications in the

Official Gazette. India has made such provision.[10] In this respect, we propose the following provision:-

"9. Electronic Gazette.- Where any law requires that any law, rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or the Electronic Gazette:

Provided that where any law, rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or the Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form."

In the Indian Act a provision has been made to the effect that notwithstanding the provisions proposed in sections 7, 8 and 9 above, no person shall have the right to compel the Government or any agency of the Government or any authority or body established by any law or controlled or funded by the Government to accept, issue, create, retain and preserve any document in the form of electronic records. In other words, the Government has been given the alternative right to perform transactions in the existing ordinary form. This provision is necessary as electronic transactions are new in this country and many Government departments still lack the logistics to perform transactions in electronic form. In this context, the Indian provision may be adopted. It is, accordingly, proposed as follows:-

"10. No liability on Government to accept documents in electronic form.- Nothing contained in this Act shall by itself compel any Ministry or Department of the Government or any authority or body established by or under any law or controlled or funded by the Government to accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form."

[10] (Indian) Information Technology Act, 2000, section 8.

Next, the Government may be empowered to make rules in respect of certain matters of digital signatures.

"11. Power of Government to make rules in respect of digital signatures.- The Government may, by notification in the Official Gazette, make rules to prescribe for the purposes of this Act-

(a) the type of digital signature;

(b) the manner and format in which the digital signature shall be affixed;

(c) the manner or procedure which facilitates identification of the person affixing the digital signature;

(d) the control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(e) any other matter which is necessary to give legal effect to digital signatures."

Next comes the concept of attribution. Very often, data messages are generated automatically by computers without direct human intervention. The computers are programmed by the originator to do this. In the case of a paper-based communication a problem may arise as the result of an alleged forged signature of the purported originator. In an electronic environment, an unauthorised person may have sent the message but the authentication by code or like manner would be accurate. There should, therefore, be provision laying down the criteria or principles of attribution establishing a presumption that under certain circumstances a data message would be considered as a message of the originator. There should also be provision to qualify the presumption in case the addressee knew or ought to have known that the data message was not that of the originator. The principles of attribution as laid down in the UNCITRAL Model Law are as follows:-

(a) A data message is considered to be that of the originator if it was sent by the originator itself.

(b) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent (i) by a person who had the authority to act on behalf of the originator in respect of that data message; or (ii) by an information system programmed by, or on behalf of, the originator automatically.

(c) As between the originator and the addressee, an addressee is entitled to regard the data message as being that of the originator, and to act on that assumption if (i) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or (ii) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.[11]

In the Model Law certain exceptions have been made to the above rules.

In Singapore, the principles laid down in the Model Law have been adopted almost in verbatim.[12]

India has adopted the principles of the Model law in part and without the exceptions. It appears that only paras 1 and 2 of Article 13 of the Model Law have been adopted by India.[13]

It appears to us that the entire principles of the Model Law may be adopted as in Singapore.

So, the next provision may be as follows:-

[11] UNCITRAL Model Law, Article 13.
[12] (Singapore) Electronic Transactions Act, 1998, section 13.
[13] 9Indian) Information Technology Act, 2000, section 11.

Chapter III

ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS

"12. Attribution.- (1) An electronic record shall be that of the originator if it was sent by the originator himself.

(2) As between the originator and the addressee, an electronic record shall be deemed to be that of the originator if it was sent-

(a) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(b) by an information system programmed by or on behalf of the originator to operate automatically.

(3) As between the originator and the addressee, an addressee shall be entitled to regard an electronic record as being that of the originator and to act on that assumption if-

(a) in order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the information as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify the electronic records as its own.

(4) Sub-section (3) of this section shall not apply-

(a) from the time when the addressee has received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly;

(b) in such case as in clause (b) of section (3) of this section, at any time when the addressee knew or ought to have known, after using

reasonable care or using any agreed procedure, that the electronic record was not that of the originator; or

(c) if, in all circumstances of the case, it is unconscionable for the addressee to regard the electronic record as being that of the originator or to act on that assumption.

(5) Where an electronic record is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee shall be entitled to regard the electronic record received as being what the originator intended to send, and to act on that assumption:

Provided that the addressee shall not be so entitled when the addressee knew or should have known, after exercising reasonable care or using any agreed procedure, that the transmission resulted in any error in the electronic record as received.

(6) The addressee shall be entitled to regard each electronic record received as separate electronic record and to act on that assumption, except to the extent that the addressee duplicates another electronic record and the addressee knew or should have known, after exercising reasonable care or using any agreed procedure, that the electronic record was a duplicate."

The next provision should deal with acknowledgement of receipt of electronic records. The principles of acknowledgement of receipt of electronic records or data message have been laid down in the Model law and India and Singapore have adopted these principles.[14] Following the principles laid down in the Model Law, we propose the next provision as follows:-

"13. Acknowledgement of receipt.- (1) Sub-sections (2) (3) and (4) of this section shall apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.

[14] UNCITRAL Model Law, Article 14; (Indian) Information Technology Act, 2000, section 12; (Singapore) Electronic Transactions Act, 1998, section 14.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by –

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(3) Where the originator has stipulated that the electronic record shall be conditional on receipt of the acknowledgement, then, until the acknowledgement has been received, the electronic record shall be deemed to have been never sent by the originator.

(4) Where the originator has not stipulated that the electronic record shall be conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator-

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if no acknowledgement is received within the time specified in clause (a) of this sub-section, may, after giving notice to the addressee, treat the electronic record as though it has never been sent.

(5) Where the originator receives the addressee's acknowledgement of receipt, it shall be presumed that the related electronic record was received by the addressee, but that presumption shall not imply that the content of the electronic record corresponds to the content of the record received.

(6) Where the received acknowledgement states that the related electronic record met technical requirements, either agreed upon or set forth in

applicable standards, it shall be presumed that those requirements have been met."

For the operation of many existing laws, it is important to ascertain the time and place of despatch and receipt of information. The use of electronic communication techniques makes these difficult to ascertain. In addition, the location of certain communication systems may change without either of the parties being aware of the change. Therefore, the proposed Act should reflect the fact that the location of information systems is irrelevant and should set forth a more objective criterion, namely, the place of business of the parties. The proposed Act should, therefore, define the time of despatch of an electronic record as the time when the electronic record enters the computer resource outside the control of the originator which may either be the computer resource of an intermediary or a computer resource of the addressee. For determining the time of receipt also the proposed Act should lay down some principles.

In the Model Law the principles regarding the time, place of despatch of electronic records and place of receipt of electronic records have been laid down.[15] India and Singapore have exactly followed the principles of the Model Law. Bangladesh has no reason to make a departure. We, accordingly, propose the provisions regarding the time and place of despatch and receipt of electronic records as follows:-

"14. Time and place of despatch and receipt of electronic record.- (1) Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Save as otherwise agreed to between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely:-

[15] UNCITRAL Model Law, Article 15.

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records, receipt occurs,-

(i) at the time when the electronic record enters the designated computer resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not designated computer resource, at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) of this section shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3) of this section.

(5) For the purposes of this section,-

(a) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;

(b) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

Explanation.- "usual place of residence", in relation to a body corporate, means the place where it is registered."

In the next place, we propose to deal with secure electronic records and digital signatures. Normal and conventional handwritten signatures may perform various functions such as:-

(a) to identify a person;

(b) to provide certainty and proof as to the involvement of a person in the act of signing;

(c) to associate and connect the signer with the contents of a document;

(d) to establish the signer's intention that something has legal effect; or

(e) to show the intent of a person to associate himself with the content of a document written by someone else.

So, an electronic or a digital signature should be so designed as to be able to achieve all the above objects of conventional paper based signatures and should be "functional equivalent" of conventional signatures. There must be a proper security method for ensuring the acceptability of an electronic signature. The following factors are required to be taken into account in determining whether the security method used for an electronic signature is appropriate, legal, technical and commercial:- (a) the sophistication of the equipment used by each of the parties; (b) the nature of their trade activity; (c) the frequency at which commercial transactions take place between the parties; (d) the kind and size of the transaction; (e) the function of signature requirements in a given regulatory and statutory environment; (f) the capability of communication systems; (g) compliance with authentication procedures set forth by intermediaries; (h) the range of authentication procedures made available by the intermediary; (i) compliance with trade customs and practice; (j) the existence of insurance coverage mechanisms against unauthorised messages; (k) the importance and the value of the information contained in the electronic record; (l) the availability of alternative methods of identification and the cost of implementation; (m) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the

method was agreed upon and the time when the electronic record was communicated and (n) any other relevant factor. In order to achieve the basic purposes of signatures, the following effects are needed:- (a) signature authentication; (b) document authentication i.e. a signature should identify what is signed and make it impracticable to falsify or alter either the signed matter or the signature; (c) affirmative act i.e. to serve the ceremonial and approval functions of a signature, a person should be able to create a signature to mark an event, indicate approval and authorisation and establish the sense of having legally consummated a transaction and (d) efficiency i.e. optimally, a signature and its creation and verification processes should provide the greatest possible assurance of authenticity and validity with the least possible expenditure of resources.

In the following sections provisions are proposed to reflect the above principles:-

Chapter IV

SECURE ELECTRONIC RECORDS & SECURE DIGITAL SIGNATURES

"15. Secure electronic record.- Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

16. Secure digital signature.- If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was-

(a) unique to the person affixing it;

(b) capable of identifying the person affixing it;

(c) created in a manner or using a means under the sole control of the person affixing it; and

(d) is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated,

then such digital signature shall be deemed to be a secure digital signature.

17. Security procedure.- The Government shall, for the purposes of this Act, prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including –

(a) the nature of the transaction;

(b) the level of sophistication of the parties with reference to their technological capacity;

(c) the volume of similar transactions engaged in by other parties;

(d) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and

(f) the procedures in general use for similar types of transactions or communications."

The next provisions should deal with certifying authorities. A certifying authority can be defined as an authority whose functions are to:-

(a) reliably identify persons applying for signature key certificates;

(b) reliably verify their legal capacity;

(c) confirm the attribution of a public signature key to an identified physical person by means of a signature key certificate;

(d) always maintain the on-line access to the signature key certificates with the agreement of the signature key owner; and

(e) take measures so that the confidentiality of a private signature key is guaranteed.

Some of the services which a certifying authority may provide can be:-

(a) managing cryptographic keys used for digital signatures;

(b) certifying that a public key corresponds to a private key;

(c) providing keys to end users;

(d) deciding which users will have which privileges on the system;

(e) publishing a secure directory of public keys or certificates;

(f) managing personal tokens (e.g. smart cards) that can identify the user with unique personal identification information or can generate or store an individual's private keys;

(g) checking the identification of end users and providing them with services;

(h) providing non-repudiation services;

(i) providing time-stamping services; and

(j) managing encryption keys used for confidentiality encryption where the use of such a technique is authorised.

In many countries certifying authorities are organised hierarchically and is technically named public key infrastructure (PKI). We propose to follow the same structure of certifying authorities. In the next place, the certifying authorities are required to maintain certain requirements, such as, independence, internal security, longevity, financial resources, legal service, contingent plan, proved experience and proficiency in information technology, particularly, in encryption and decryption technologies and familiarity with security procedures, protection arrangement for its own private key, revocation procedures, insurance, inter-operationality with other national and foreign certification authorities, personnel selection and reliable management. The above matters are required to be regulated by the chief of the certifying authorities. Keeping the above aspects in mind, we propose the provisions regarding the certifying authorities as follows:-

Chapter V

CONTROLLER & CERTIFYING AUTHORITIES

“18. Certifying Authorities Controller and other officers.- (1) The Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act.

(2) The Government may, by notification in the Official Gazette, also appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.

(3) The Controller shall discharge such functions as are vested in him under this Act under the general superintendence and control of the Government.

(4) The Deputy Controllers and the Assistant Controllers shall perform such functions as are assigned to them by the Controller under the general superintendence and control of the Controller.

(5) The qualifications, experience and terms and conditions of service of the Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Government.

(6) The Head Office and Branch Offices of the office of the Controller shall be at such places as the Government may specify and may be established at such places as the Government may think fit.

(7) There shall be a seal of the office of the Controller as the Government may specify.

19. Functions of the Controller. - The Controller may perform all or any of the following functions, namely:-

(a) exercising supervision over the activities of the Certifying Authorities;

(b) certifying public keys of the Certifying Authorities;

(c) laying down the standards to be maintained by the Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certifying and the public key;

(g) specifying the form and content of a Digital Signature Certificate and the key;

(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such system;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a database containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to the members of the public.

20. Recognition of foreign Certifying Authorities.- (1) Subject to such conditions and restrictions as may be specified, by regulations, the Controller may, with the previous approval of the Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognised under sub-section (1) of this section, the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may, if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) of this section, he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

21. Controller to act as repository.- (1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.

(2) The Controller shall ensure that the secrecy and security of the digital signatures are assured and in order to do so shall –

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) observe such other standards as may be prescribed by the Government.

(3) The Controller shall maintain a computerised database of all public keys in such a manner that such database and the public keys are available to any member of the public.

22. Licence to issue Digital Signature Certificates.- (1) Subject to the provisions of sub-section (2) of this section, any person may make an application to the Controller for a licence to issue Digital Signature Certificates.

(2) No licence shall be issued under sub-section (1) of this section unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities which are necessary to issue Digital Signature Certificates as may be prescribed by the Government.

(3) A licence granted under sub-section (1) of this section –

(a) shall be valid for such period as may be prescribed by the Government;

(b) shall be subject to such terms and conditions as may be specified by the Controller; and

(c) shall not be transferable or heritable.

23. Application for licence.- (1) Every application for issue of a licence shall be in such form as may be prescribed by the Government.

(2) Every application for issue of a licence shall be accompanied by –

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding taka twenty-five thousand, as may be prescribed by the Government; and

(d) such other documents as may be prescribed by the Government.

24. Renewal of licence.- (1) An application for renewal of a licence shall be in such form as may be prescribed by the Government.

(2) Every application for renewal of a licence shall be accompanied by such fees, not exceeding taka twenty five thousand, as may be prescribed by the Government.

(3) Every application for renewal of a licence shall be made not less than forty five days before the date of expiry of the period of validity of the licence.

25. Procedure for grant or rejection of licence.- The Controller may, on receipt of an application under sub-section (1) of section 22 of this Act, after considering the documents accompanying the application and such other factors as he deems fit, grant the licence or reject the application:

Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

26. Revocation and suspension of licence.- (1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has –

(a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

(c) failed to maintain the standards specified under clause (b) of sub-section (2) of section 21 of this Act;

(d) contravened any provisions of this Act, rules, regulations or orders made thereunder;

revoke the licence:

Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1) of this section, by order, suspend such licence pending the completion of any enquiry ordered by him:

Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) A Certifying Authority whose licence has been suspended shall not issue any Digital Signature Certificate during the period of such suspension.

27. Notice of revocation or suspension of licence.- (1) Where the licence of a Certifying Authority is revoked or suspended, the Controller shall publish notice of such revocation or suspension, as the case may be, in the database maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such revocation or suspension, as the case may be, in all such repositories:

Provided that the database containing the notice of such revocation or suspension, as the case may be, shall be made available through a website which shall be accessible round the clock:

Provided further that the Controller may, if he considers necessary, publicise the contents of database in such electronic or other media as he may consider appropriate.

28. Power to delegate.- The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any other officer to exercise any of the powers of the Controller under this Chapter.

29. Power to investigate contraventions.- (1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall, for the purposes of sub-section (1) of this section, have the same powers as are vested in a Civil Court under the Code of Civil Procedure, 1908, (Act V of 1908), when trying a suit in respect of the following matters, namely:-

(a) discovery and inspection;

(b) enforcing the attendance of any person and examining him on oath or affirmation;

(c) compelling the production of any documents; and

(d) issuing commissions for the examination of witness.

30. Access to computers and data.- (1) Without prejudice to the provisions of section 71 of this Act, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act or rules and regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purpose of sub-section (1) of this section, the Controller or any person authorised by him may, by order, direct any person in charge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

31. Certifying Authority to follow certain procedures.- Every Certifying Authority shall, -

(a) make use of hardware, software, and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) observe such other standards as may be specified by regulations.

32. Certifying Authority to ensure compliance of the Act, rules, regulations, etc.- Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations or orders made thereunder.

33. Display of licence.- Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carriers on its business.

34. Surrender of licence.- Every Certifying Authority whose licence is revoked or suspended shall immediately after such revocation or suspension, surrender the licence to the Controller.

35. Disclosure.- (1) Every Certifying Authority shall disclose in the manner specified by regulations –

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Certifying Authority has issued, or the Certifying Authority's ability to perform its services.

(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall –

(a) use reasonable efforts to notify any person who is likely to be affected by the occurrence; or

(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

36. Issue of certificate.- (1) The Certifying Authority may issue a certificate to a prospective subscriber only after the Certifying Authority –

(a) has received an application in the prescribed form requesting for issuance of a certificate from the prospective subscriber; and

(b) has –

(i) if it has a certification practice statement, complied with all of the practices and procedures set forth in such certification practice statement including procedures regarding identification of the prospective subscriber; or

(ii) in the absence of a certification practice statement, the Certifying Authority shall confirm by itself or through an authorised agent that –

(a) the prospective subscriber is the person to be listed in the certificate to be issued;

(b) if the prospective subscriber is acting through one or more agents, the subscriber authroised the agent to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(c) the information in the certificate to be issued is accurate;

(d) the prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(e) the prospective subscriber holds a private key capable of creating a digital signature; and

(f) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber.

(2) The prospective subscriber shall pay such fees as may be prescribed for issuance of a certificate.

37. Representations upon issuance of certificate.- (1) By issuing a certificate, the Certifying Authority represents to any person who reasonably relies on the certificate or a digital signature verifiable by the public key listed in the certificate that the Certifying Authority has issued the certificate in accordance with any applicable certification practice statement incorporated by reference in the certificate, or of which the relying person has notice.

(2) In the absence of such certification practice statement, the Certifying Authority represents that it has confirmed that –

(a) the Certifying Authority has complied with all applicable requirements of this Act and the rules and regulations made thereunder in issuing the certificate, and if the Certifying Authority has published the certificate or otherwise made it available to such relying person, that the subscriber listed in the certificate has accepted it;

(b) the subscriber identified in the certificate holds the private key corresponding to the public key listed in the certificate;

(c) the subscriber's public key and private key constitute a functioning key pair;

(d) all information in the certificate is accurate, unless the Certifying Authority has stated in the certificate or incorporated by reference in the certificate a statement that the accuracy of specified information is not confirmed; and

(e) the Certifying Authority has no knowledge of any material fact which if it had been included in the certificate would adversely affect the reliability of the representations in clauses (a) to (d) of this sub-section.

(3) Where there is an applicable certification practice statement which has been incorporated by reference in the certificate, or of which the relying person has notice, sub-section (2) of this section shall apply to the extent that the representations are not inconsistent with the certification practice statement.

38. Revocation of Digital Signature Certificate.- (1) A Certifying Authority shall revoke a Digital Signature Certificate issued by it –

(a) where the subscriber or any person authorised by him makes a request to that effect; or

(b) upon the death of the subscriber;

(c) where the subscriber is a firm or a company, if it has been dissolved or wound up or has otherwise ceased to exist.

(2) Subject to the provisions of sub-section (3) of this section and without prejudice to the provisions of sub-section (1) of this section, a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time if it is of opinion that –

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent by a competent court or authority.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

39. Suspension of Digital Signature Certificate.- (1) Subject to the provisions of sub-section (2) of this section, the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,-

(a) on receipt of a request to that effect from –

(i) the subscriber listed in the Digital Signature Certificate; or

(ii) any person duly authorised to act on behalf of that subscriber;

(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.

(2) A Digital Signature Certificate shall not be suspended for a period exceeding thirty days without giving the subscriber an opportunity of being heard in the matter.

(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

40. Notice of revocation or suspension.- (1) Where a Digital Signature Certificate is revoked under section 38 of this Act or suspended under section 39 of this Act, the Certifying Authority shall publish a notice of such revocation or suspension, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such revocation or suspension, as the case may be, in all such repositories."

In the next provisions we propose to deal with the duties of subscribers in electronic transactions. The provisions in this respect in India and Singapore are substantially almost identical – the difference lies only in the choice of words and framing of the sections. We propose these provisions as follows:-

Chapter VI

DUTIES OF SUBSCRIBERS

"41. Generating key pair.- If the subscriber generates the key pair whose public key is to be listed in a Digital Signature Certificate issued by a Certifying Authority and accepted by the subscriber, the subscriber shall generate the key pair by applying the security procedure.

42. Acceptance of Digital Signature Certificate.- (1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he

(a) publishes or authorises the publication of a Digital Signature Certificate–

(i) to one or more persons; or

(ii) in a repository; or

(b) otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all materials relevant to the information contained in the Digital Signature Certificate are true; and

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

43. Obtaining Digital Signature Certificate.- All material representations made by the subscriber to a Certifying Authority for purposes of obtaining a certificate, including all information known to the subscriber and represented in

the Digital Signature Certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the Certifying Authority.

44. Control of private key.- (1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority who has issued the Digital Signature Certificate in such manner as may be specified by regulations.

Explanation.- For the purpose of removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised."

After the above provisions, contraventions and information technology offences are required to be dealt with.

Certain computer-related unauthorized and harmful acts primarily involve liability of civil nature and these acts may be categorized as "contraventions" for which imposition of penalty/ compensation/ damage etc. would be sufficient. For dealing with "contraventions" some countries have made provisions for establishment of special forums as well as appellate forums as their adjudication may require expert knowledge. Some other computer-related harmful acts of more serious nature have been specified as penal offences made punishable with imprisonment, fines, etc. and triable by criminal courts.

The acts constituting "contraventions' may be categorized as follows:-

(a) accessing or securing access to the computer or computer network;

(b) downloading any data or information from the computer or computer network;

(c) introducing or causing to be introduced any computer contaminant or computer virus into the computer or computer network;

(d) damaging or causing to be damaged the computer, computer network, data, computer database or any other programmes residing in it;

(e) disrupting or causing the disruption of the computer or computer network;

(f) denying or causing the denial of access to any person authorised to access the computer or computer network by any means;

(g) providing assistance to any person to facilitate access to the computer or computer network in contravention of the provisions of the proposed Act and rules or regulations made thereunder; and

(h) charging the services availed of by a person to the account of another person by tampering with or manipulating any computer or computer network.

The above harmful acts are popularly called "cyber vandalism", "hacking", "malicious spreading of viruses", "password fraud", etc.

In addition, the following "failures" may be included in this category:-

(i) failure to furnish documents, returns, reports, etc under the Act, rules, regulations, etc.;

(j) failure to file return, information, etc. and

(k) failure to maintain books, accounts, returns, etc.

Any person contravening any of the above clauses should be saddled with punishments which may take the form of compensation, damage, penalty, etc., or a combination of some or all of them according to the nature and gravity of the "contravention". So, we propose the following provisions

specifying the "contraventions", compensation/ penalties therefor and establishment of forums for dealing with them:-

Chapter VII

PENALTIES AND ADJUDICATION

"45. Penalty for damage to computer, computer system, etc.- If any person, without permission of the owner or any other person who is in charge of a computer, computer system or computer network,-

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention

of the provisions of this Act, or rules and regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network,

he shall be liable to pay to the person affected compensation not exceeding Taka one crore.

Explanation.- For the purposes of this section,-

(i) "computer contaminant" means any set of computer instructions that are designed-

(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system or computer network;

(ii) "computer database" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or re-arrange any computer resource by any means.

46. Penalty for failure to furnish document, return or report.- Whoever fails to furnish any document, return or report to the Controller or the Certifying Authority which he is required under this Act, or rules or regulations made thereunder to furnish shall be liable to pay a penalty which may extend to Taka two lakhs for each such failure.

47. Penalty for failure to file return, information, books, etc.- Whoever fails to file any return or furnish any information, books or other documents within the time specified therefor in this Act, or rules or regulations made thereunder shall be liable to pay a penalty which may extend to Taka ten thousand for every day during which such failure continues.

48. Penalty for failure to maintain books of accounts or records.- Whoever fails to maintain books of account or records which he is required under this Act, or rules or regulations made thereunder to maintain shall be liable to pay a penalty which may extend to Taka ten thousand for every day during which the failure continues.

49. Residuary penalty.- Whoever contravenes any provisins of this Act, or any rules or regulations made thereunder, for which no penalty has been separately provided, shall be liable to pay a compensation which may extend to Taka twenty five thousand to the person affected by such contravention or a penalty which may extend to Taka twenty five thousand.

50. Adjudicating Officer.- (1) For the purpose of adjudging whether any person has committed a contravention of any of the provisions of this Act, or of any rules or regulations made thereunder the Government shall, subject to the provisions of sub-section (2) of this section, appoint any person to be an Adjudicating Officer.

(2) No person shall be appointed as an Adjudicating Officer unless he possesses such qualifications, experience in the field of information technology, legal experience or judicial experience as may be prescribed.

(3) The Government may appoint more than one Adjudicating Officer and where more than one adjudicating officer are appointed the Government shall specify by order the matters and places with respect to which such officers shall exercise jurisdiction.

51. Powers of Adjudicating Officer.- (1) The Adjudicating Officer may, if after giving to the person referred to in sub-section (1) of section 50 of this Act a reasonable opportunity of being heard and after holding such inquiry as he may deem fit, finds that the person has committed the contravention, impose upon him such penalty or such compensation as he thinks fit, in accordance with the provisions of this Act.

(2) While adjudging the quantum of compensation or penalty, as the case may be, the Adjudicating Officer shall have due regard to the following factors, namely:-

(a) the amount of gain or unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default;

(3) Every Adjudicating Officer shall have, for the purposes of discharging his functions under this Act, the same powers as are vested in a Civil Court under the Code of Civil Procedure, 1908 (Act V of 1908), while trying a suit, in respect of the following matters, namely:-

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery, inspection and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it exparte;

(g) any other matter which may be prescribed.

(4) Subject to sub-section (3) of this section, the Adjudicating Officer shall not be bound by the procedure laid in the Code of Civil Procedure, 1908 (Act V of 1908), but shall be guided by the principles of natural justice and, subject to the provisions of this Act, or any rules or regulations made thereunder, shall have the powers to regulate its own procedure.

(5) All proceedings before the Adjudicating Officer shall be deemed to be judicial proceedings within the meaning of sections 193 and 228, and for the purposes of section 196 of the Penal Code, 1860 (Act XL of 1860).

(6) Every Adjudicating Officer shall be deemed to be a Civil Court for the purposes of section 195 and Chapter XXXV of the Code of Criminal Procedure, 1898 (Act V of 1898)."

The next provisions should deal with establishment of an appellate authority to hear appeals from the orders of the Controller of Certifying Authorities and the Adjudicating Officers. In the Indian Act, such provisions have been made.[16] There should also be provisions for appeal against the orders of the appellate authorities. To our view, appeals from the orders of the appellate authorities should lie to the High Court Division. In India, such appeals lie to the High Court.[17]

We, accordingly, propose the provisions regarding the appellate authorities as follows:-

Chapter VIII

CYBER REGULATIONS APPELLATE TRIBUNAL

"52. Establishment of Cyber Appellate Tribunal.- (1) The Government shall, by notification in the Official Gazette, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.

[16] (Indian) Information Technology Act, 2000, sections 48 to 64.
[17] Ibid, section 62.

(2) The Government shall specify, in the notification referred to in sub-section (1) of this section, the matters and places in respect of which the Cyber Appellate Tribunal may exercise jurisdiction.

53. Composition, qualifications, term of office, conditions of servcice, etc. of Cyber Appellate Tribunal.- (1) The Cyber Appellate Tribunal shall consist of one person (hereinafter referred to as the Presiding Officer) to be appointed by the Government by notification in the Official Gazette.

(2) A person shall not be qualified for appointment as the Presiding Officer of a Cyber Appellate Tribunal unless he –

(a) is, or has been, or is qualified to be, a Judge of the Supreme Court; or

(b) is, or has been, an officer in the service of the Republic not below the rank of a Secretary to the Government.

(3) The Presiding Officer of a Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age seventy two years, whichever is earlier.

(4) The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Presiding Officer of a Cyber Appellate Tribunal shall be such as may be determined by the Government.

(5) The salary and allowances and the other terms and conditions of service of the Presiding Officer of a Cyber Appellate Tribunal shall not be varied to his disadvantage during the tenure of his office.

54. Filling up of vacancies.- If any vacancy, other than temporary absence, occurs in the office of the Presiding Officer of a Cyber Appellate Tribunal, then the Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

55. Resignation and removal.- (1) The Presiding Officer of a Cyber Appellate Tribunal may resign his office by notice in writing under his hand addressed to the Government:

Provided that the said Presiding Officer shall, unless he is permitted by the Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice by the Government or until a person appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Presiding Officer of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Government on the ground of proved misconduct or physical or mental infirmity after an enquiry by a Judge of the Supreme Court nominated by the Chief Justice of Bangladesh after affording the Presiding Officer a reasonable opportunity of being heard in respect of the charges levelled against him.

(3) The Government may make rules for regulating the procedure for the enquiry under sub-section (2) of this section.

56. Orders constituting Cyber Appellate Tribunal to be final and not to invalidate proceedings.- The order of the Government appointing any person as the Presiding Officer of a Cyber Appellate Tribunal shall be final and shall not be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

57. Staff of Cyber Appellate Tribunal.- (1) The Government shall provide a Cyber Appellate Tribunal with such officers and employees as the Government may think fit.

(2) The officers and employees of a Cyber Appellate Tribunal shall be under the general control and superintendence of the Presiding Officer.

(3) The salaries, allowances and other terms and conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be determined by the Government.

58. Appeal to Cyber Appellate Tribunal.- (1) Any person aggrieved by an order made by the Controller or an Adjudicating Officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter:

Provided that no appeal shall lie to the Cyber Appellate Tribunal from an order made by an Adjudicating Officer with the consent of the parties.

(2) Every appeal under sub-section (1) of this section shall be filed within a period of 30 days from the date on which a copy of the order appealed against is received by the person aggrieved and it shall be in such form and accompanied by such fee as may be prescribed:

Provided that section 5 of the Limitation Act, 1908 (Act IX of 1908) shall apply to an appeal under this section.

(3) On receipt of an appeal under sub-section (1) of this section, the Cyber Appellate Tribunal shall, after giving the parties to the appeal reasonable opportunity of being heard, pass such orders as it may deem fit and may, by such order, confirm, modify or set aside the order appealed against or send back the matter for rehearing to the Controller or the Adjudicating Officer concerned, as the case may be.

(4) The Cyber Appellate Tribunal shall send a copy of every order made by it to the Controller or the Adjudicating Officer concerned, as the case may be.

(5) The Cyber Appellate Tribunal shall furnish copy of every order made by it to the parties to the appeal and to any other person interested on application being made to it and on payment of such fees as may be prescribed.

(6) Every appeal filed under sub-section (1) of this section shall be disposed of by the Cyber Appellate Tribunal as expeditiously as possible and

every endeavour shall be made for its disposal within a period of six months from the date of its receipt.

59. Procedure and powers of Cyber Appellate Tribunal.- (1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down in the Code of Civil Procedure, 1908 (Act V of 1908), but shall be guided by the principles of natural justice and, subject to the provisions of this Act and of any rules and regulations made thereunder, shall have the powers to regulate its own procedure including determination of the place or places at which it shall hold its sittings.

(2) Notwithstanding sub-section (1) of this section, the Cyber Appellate Tribunal shall have the same powers as are vested in a Civil Court under the Code of Civil Procedure, 1908 (Act V of 1908), while trying a suit, in the following matters, namely:-

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery, inspection and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commission for the examination of witnesses or documents;

(e) reviewing its decision;

(f) dismissing an application for default or deciding it exparte;

(g) any other matter which may be prescribed.

(3) All proceedings before a Cyber Appellate Tribunal shall be deemed to be judicial proceedings within the meaning of sections 193 and 228, and for the purposes of sections 196 of the Penal Code, 1860 (Act XLV of 1860) and a Cyber Appellate Tribunal shall be deemed to be a Civil Court for the purposes of section 195 and Chapter XXXV of the Code of Criminal Procedure, 1898 (Act V of 1898).

60. Right of legal representation.- The parties to an appeal may either appear in person or authorise one or more legal practitioners or any of their officers to present their cases before the Cyber Appellate Tribunal.

61. Application of the Limitation Act 1908 (Act IX of 1908).- Subject to the provisions of this Act, the provisions of the Limitation Act, 1908 (Act IX of 1908) shall, as far as may be applicable, apply to an appeal filed under sub-section (1) of section 58 of this Act.

62. Court's jurisdiction barred.- Save as is provided in this Act, no court shall entertain any suit or proceeding in respect of any matter which an Adjudicating Officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in exercise of any power conferred by or under this Act.

63. Appeal to High Court Division.- Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal against such decision or order to the High Court Division within sixty days from the date of receipt of the copy of the decision or order of the Cyber Appellate Tribunal on any question of fact or law:

Provided that section 5 of the Limitation Act, 1908 (Act IX of 1908) shall apply to an appeal under this section.

64. Compounding of contraventions.- (1) Any contravention under this Act may, either before or after the institution of adjudication proceedings, be compounded by the Controller or such other officer as may be authorised by him in this behalf or by the Adjudicating Officer, as the case may be, subject to such conditions as the Controller or such other officer or the Adjudicating Officer may specify:

Provided that if the condition specified is payment of any sum of money by one party to the other, such sum shall not, in any case, exceed the maximum

amount of penalty which may be imposed under this Act for the contravention so compounded.

(2) Nothing in sub-section (1) of this section shall apply to a person who commits the same or similar contravention within a period of three years from the date on which the first contravention, committed by him, was compounded.

Explanation.- For the purposes of this sub-section, any second or subsequent contravention committed after the expiry of a period of three years from the date on which the contravention was previously compounded shall be deemed to be a first contravention.

(3) Where any contravention has been compounded under sub-section (1) of this section, no proceeding or further proceeding, as the case may be, shall be taken against the person guilty of such contravention in respect of the contravention so compounded.

65. Recovery of penalty and compensation.- Any penalty or compensation payable under this Act, if not paid, shall be recoverable as arrear of land revenue and the licence or the Digital Signature Certificate, as the case may be, of the defaulter shall be suspended till the penalty or the compensation, as the case may be, is paid."

We next propose to deal with information technology offences and punishments for such offences.

While dealing with offences in the working paper we did not consider a very important aspect. Now-a-days computers are being used by criminals for committing various types of offences including offences of very serious nature. Many such offences are included in our penal laws such as, the Penal Code, 1860, the Special Powers Act, 1974, etc. etc. In a recent conference organised by the United States Department of Justice on Legal Framework for Combating Cybercrime held in Moscow on 17-18 August, 2002, use of computers for committing various types of criminal offences and as to how to combat it was highlighted and the discussion mainly centered round commission of terrorist

acts by various terrorist groups around the world. Speakers from various countries emphasized the need for making use of computers for committing terrorist acts an offence. Some delegates pointed out that there is no unanimity among nations on the definition of terrorism and in the penal laws of many countries the term, "terrorism", does not appear as an offence. It is, however, necessary to prevent use of computers for any penal offence whatsoever. In the working paper no proposal has been made for including use of computers for committing an offence as a punishable offence. So, a new section may be added making the use of computers for committing an offence as a punishable offence under the proposed Act and in this connection, the term "act" and "offence", will require definition. So, the offences relating to information technology may be classified as follows:- (a) Source code attacks; (b) Hacking; (c) Obscenity; (d) Failure to comply with Controller's directions; (e) Subscriber's failure to comply with Controller's requirement for decryption; (f) Accessing designated protected systems; (g) Misrepresentation to the Controller; (h) Breach of confidentiality or privacy; (i) Publishing False Digital Signature Certificate; (j) Making available Digital Signature for fraudulent purposes and (k) Use of computers for committing an offence. Specific punishments should be provided for these offences in the proposed Act. Moreover, in addition to punishments, provisions for confiscation of computers, computer system, floppies, compact disks, tape drives or any other accessories related thereto in respect of which contravention or offence occurs should be made but there may be exceptions for those who are found to be innocent. Penalty, compensation and confiscation should also be in addition to punishments for offences. We, accordingly, propose the next provisions as follows:-

Chapter IX

OFFENCES

"66. Punishment for tampering with computer source documents.- Whoever intentionally or knowingly conceals, destroys or alters or

intentionally or knowingly causes any other person to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by any law for the time being in force, shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka two lakhs, or with both.

Explanation.- For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

67. Hacking with computer system.- Whoever, with intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits the offence of "hacking".

68. Punishment for hacking.- Whoever commits hacking shall be punished with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka two lakhs, or with both.

69. Punishment for publishing obscene information in electronic form.- Whoever publishes or transmits or causes to be published or transmitted in electronic form any material which is obscene or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to Taka one lakh and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and with fine which may extend to Taka two lakhs for each such subsequent offence.

70. Punishment for failure to surrender licence under section 34.- Where any Certifying Authority fails to surrender a licence under section 34 of this Act, the person in whose favour the licence is issued shall be guilty of an offence and shall be punished with imprisonment of either description for a term which may extend to six months or with fine which may extend to Taka ten thousand or with both.

71. Power of Controller to give directions.- The Controller may, by order, direct a Certifying Authority or any employee of such a Certifying Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, or rules and regulations made thereunder.

72. Punishment for failure to comply with order made under section 71.- Any person who fails to comply with any order made under section 71 of this Act shall be guilty of an offence and shall be liable on conviction to suffer imprisonment of either description for a term which may extend to one year or to pay a fine which may extend to Taka one lakh or to both.

73. Directions of Controller to a subscriber to extend facilities to decrypt information.- (1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty, integrity, or security of Bangladesh, friendly relations of Bangladesh with other States, public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in charge of a computer resource shall, when called upon by any agency to which direction has been issued under sub-section (1) of this section, extend all facilities and technical assistance to decrypt the information.

74. Punishment for failure to comply with sub-section (2) of section 73.- The subscriber or any person who fails to assist the agency referred to in sub-section (2) of section 73 of this Act shall be punished with imprisonment of

either description for a term which may extend to seven years or with fine which may extend to Taka one lakh or with both.

75. Protected system.- (1) The Government may, by notification in the Official Gazette, declare any computer, computer system or computer network to be a protected system.

(2) The Government may, by order in writing, authorise the persons who are authorised to secure access to protected systems notified under sub-section (1) of this section.

76. Punishment for unauthorised access to protected systems.- Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of section 75 of this Act shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine which may extend to Taka two lakhs.

77. Punishment for misrepresentation.- Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be, shall be punished with imprisonment of either description for a term which may extend two years, or with fine which may extend to Taka one lakh, or with both.

78. Bar on disclosure of confidentiality and privacy.- Save as otherwise provided by this Act or any other law for the time being in force, no person who, in pursuance of any of the powers conferred under this Act, or rules and regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material shall, without the consent of the person concerned, disclose such electronic record, book, register, correspondence, information, document or other material to any other person.

79. Punishment for breach of confidentiality and privacy.- Whoever contravenes the provisions of section 78 of this Act shall be punished with

imprisonment of either description for a term which may extend to two years, or with fine which may extend to Taka one lakh, or with both.

80. Bar on publishing false Digital Signature Certificate.- No person shall publish a Digital Signature Certificate or otherwise make it available to any other person knowing that –

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

81. Punishment for publishing false Digital Signature Certificate.- Whoever contravenes the provisions of section 80 of this Act shall be punished with imprisonment of either description for a term which may extend to two years, or with fine which may extend to Taka one lakh, or with both.

82. Punishment for publication for fraudulent purpose.- Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, which may extend to Taka one lakh, or with both.

83. Punishment for using computer for committing an offence.- Whoever uses or intentionally causes to be used a computer, computer network, computer resource or computer system for, or for facilitating, the commission of an offence shall be punished, if the offence has been committed, with the punishment provided for the offence and if the offence has not been committed, with imprisonment of either description for a term which may extend to half of the period of imprisonment prescribed for the offence or with fine or with both.

84. Act to apply for offence or contravention committed outside Bangladesh.- (1) Subject to the provisions of sub-section (2) of this section,

the provisions of this Act shall apply also to any offence or contravention committed outside Bangladesh by any person irrespective of his nationality.

(2) For the purposes of sub-section (1) of this section, this Act shall apply to an offence or contravention committed outside Bangladesh by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in Bangladesh.

85. Confiscation.- Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, or in respect of which any offence has been committed, shall be liable to confiscation by an order of the court trying an offence or contravention:

Provided that where it is established to the satisfaction of the court that the person in whose possession, power or control any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorised by this Act against the person contravening the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

Explanation.- For the purposes of this section, court includes Adjudicating Officer and Cyber Appellate Tribunal.

86. Penalties or confiscation no bar against other punishments.- No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby may be liable under any other law for the time being in force.

87. Power of investigation of offences under this Act.- Notwithstanding anything contained in the Code of Criminal Procedure, 1898 (Act V of 1898), a police officer not belo w the rank of an Inspector of Police shall investigate any offence under this Act."

In the Indian Act, a provision has been made to exempt an intermediary providing service from the liability of penalty or punishment for contravention of any provision of the Act if he proves that the offence or contravention was committed without his knowledge or that he had exercised due diligence to prevent the commission of such offence or contravention.[18] We may as well include such a provision in the proposed Act. The next provision may, accordingly, be as follows:-

"88. Network service providers not to be liable in certain cases.- For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, or rules and regulations made thereunder, for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised due diligence to prevent the commission of such offence or contravention.

Explanation.- For the purposes of this section,-

(a) "network service provider" means an intermediary;

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary."

Separate specific provision is required to be made for imposition of liability when offences or contraventions are committed by a company. This provision may run as follows:-

"89. Offences committed by companies.- (1) Where a person committing an offence under this Act, or rule and regulation made thereunder or a contravention of any provision of this Act, rule, regulation, direction or order

[18] (Indian) Information Technology Act, 2000, section 79.

made thereunder is a company, every person who, at the time the offence or the contravention, as the case may be, was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the offence or the contravention, as the case may be, and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person to punishment if he proves that the offence or contravention was committed without his knowledge or that he exercised due diligence in order to prevent commission of such offence or contravention.

(2) Notwithstanding anything contained in sub-section (1) of this section, where an offence under this Act, or rule and regulation made thereunder or contravention of any provision of this Act, rule, regulation, direction or order made thereunder has been committed by a company and it is proved that the offence or the contravention, as the case may be, has taken place with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence or the contravention and shall be liable to be proceeded against and punished accordingly.

Explanation.- For the purposes of this section.-

(a) "company" means any body corporate and includes a firm or other association of individuals; and

(b) "director", in relation to a firm, includes a partner in the firm."

90. Power of police officer and other officers to enter, search, etc.- (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1898 (Act V of 1898), any police officer, not below the rank of an Inspector of Police, or any other officer of the Government authorised by the Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

Explanation.- For the purposes of this sub-section, the expression, "public place", includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to, the public.

(2) Where any person is arrested under sub-section (1) of this section by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer in charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1898 (Act V of 1898) shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest made under this section."

In the concluding part of the Act, certain miscellaneous provisions are required to be made. These are: (1) overriding effect of the Act; (2) declaring certain functionaries under the Act as public servants; (3) immunity; (4) removal of difficulties; and (5) power to make rules. We propose these provisions as follows:-

Chapter X

MISCELLANEOUS

91. Act to override other laws.- The provisions of this Act shall have effect notwithstanding anything inconsistent therewith in any other law for the time being in force.

92. Presiding Officer, Controller, etc. to be public servants.- The Presiding Officer, the Controller, the Deputy Controllers, the Assistant Controllers, the Adjudicating Officers and the officers and the employees of the Cyber Appellate Tribunal, the Controller, the Deputy Controllers, the Assistant Controllers and the Adjudicating Officers shall be deemed to be public servants within the meaning of section 21 of the Penal Code, 1860 (Act XLV of 1860).

93. Protection of action taken in good faith.- No suit, prosecution or other legal proceedings shall lie against the Government, the Controller or any person acting on his behalf, the Presiding Officer of the Cyber Appellate

Tribunal, the Adjudicating Officers, and the staff of the Presiding Officer of the Cyber Appellate Tribunal, the Controller and the Adjudicating Officers for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation, order or direction made thereunder.

94. Removal of difficulties.- (1) If any difficulty arises in giving effect to the provisions of this Act, the Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as appear to it to be necessary or expedient for removing the difficulty:

Provided that no order shall be made under this sub-section after the expiry of two years from the date of commencement of this Act.

(2) Every order made under sub-section (1) of this section shall be laid, as soon as may be after it is made, before the Parliament.

95. Power of Government to make rules.- (1) The Government may, by notification in the Official Gazette and in the Electronic Gazette, make rules for carrying out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:-

(a) the manner in which any information or matter may be authenticated or any document may be signed by means of digital signature under section 6 of this Act;

(b) the electronic form in which filing, issue, grant or payment shall be effected under sub-section (1) of section 7 of this Act;

(c) the manner and format in which electronic records shall be filed, or issued and the method of payment under sub-section (2) of section 7 of this Act;

(d) the matters relating to the type of digital signature, manner and format in which it may be affixed under section 11 of this Act;

(e) the security procedure for the purpose of creating secure electronic record and secure digital signature under section 17 of this Act;

(f) the qualifications, experience and terms and conditions of service of the Controller, Deputy Controllers and Assistant Controllers under section 18 of this Act;

(g) other standards to be observed by the Controller under clause (b) of sub-section (2) of section 21 of this Act;

(h) the requirements which an applicant must fulfil under sub-section (2) of section 22 of this Act;

(i) the period of validity of licence granted under clause (a) of sub-section (3) of section 22 of this Act;

(j) the form in which an application for licence may be made under sub-section (1) of section 23 of this Act;

(k) the amount of fees payable under clause (c) of sub-section (2) of section 23 of this Act;

(l) such other documents which shall accompany an application for licence under clause (d) of sub-section (2) of section 23 of this Act;

(m) the form of application for renewal of a licence and the fee payable therefor under section 24 of this Act;

(n) the form in which application for issue of a Digital Signature Certificate may be made under clause (a) of sub-section (1) of section 36 of this Act;

(o) the fee to be paid under sub-section (2) of section 36 of this Act;

(p) the qualifications and experience which Adjudicating officer shall possess under sub-section (2) of section 50 of this Act;

(q) the manner in which the Adjudicating officer shall hold inquiry under sub-section (1) of section 51 of this Act;

(r) the procedure for inquiry into misconduct or physical or mental incapacity of the Presiding Officer under sub-section (2) of section 55 of this Act;

(s) the form in which appeal may be filed and the fee thereof under sub-section (2) of section 58 of this Act;

(t) any other power of a Civil Court required to be prescribed under clause (g) of sub-section (2) of section 59 of this Act; and

(u) any other matter which is required to be, or may be, prescribed.

(3) Every notification made by the Government under sub-section (2) of section 2 of this Act and every rule made by it shall be laid, as soon as may be after it is made, before the Parliament, while it is in session, and if the Parliament resolves that the notification or the rule should not be made, or to make any modification in the notification or the rule, the notification or the rule shall thereafter be of no effect or have effect only in such modified form, as the case may be; but, such annulment or modification shall be without prejudice to the validity of anything previously done under that notification or rule.

96. Power of Controller to make regulations.- (1) The Controller may, after consultation with the Cyber Regulations Advisory Committee constituted under section 97 of this Act and with the previous approval of the Government, by notification in the Official Gazette, make regulations consistent with the provisions of this Act and the rules made thereunder to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:-

(a) the particulars relating to maintenance of database containing the disclosure record of every Certifying Authority under clause (n) of section 19 of this Act;

(b) the conditions and restrictions subject to which the Controller may recognise any foreign Certifying Authority under sub-section (1) of section 20 of this Act;

(c) the terms and conditions subject to which a licence may be granted under clause (b) of sub-section (3) of section 22 of this Act;

(d) other standards to be observed by a Certifying Authority under clause (d) of section 31 of this Act;

(e) the manner in which the Certifying Authority shall disclose the matters specified in sub-section (1) of section 35 of this Act;

(f) the particulars of statement which shall accompany an application under sub-section (1) of section 36 of this Act;

(g) the manner by which the subscriber shall communicate the compromise of private key to the Certifying Authority under sub-section (2) of section 44 of this Act.

(3) Every regulation made under this Act shall be laid, as soon after it is made as may be, before the Parliament and if the Parliament resolves that the regulation should not be made or to make any modification in the regulation, the regulation shall thereafter be of no effect or have effect only in such modified form, as the case may be:

Provided that any such annulment or modification shall be without prejudice to the validity of anything previously done under that regulation."

In the Indian Act, provision has been made for formation of an advisory committee named as Cyber Regulations Advisory Committee for advising the Government in matters connected with the Act.[19] We may make similar provision.

"97. Cyber Regulations Advisory Committee.- (1) The Government shall, as soon after the commencement of this Act as may be, constitute a committee called the Cyber Regulations Advisory Committee.

(2) The Cyber Regulations Advisory Committee shall consist of a Chairman and such number of other official and non-official members

[19] (Indian) Information Technology Act, 2000, section 88.

representing the interests principally affected or having special knowledge of the subject-matter as the Government may deem fit.

(3) The Cyber Regulations Advisory Committee shall advice –

(a) the Government either generally as regards any rules or for any other purpose connected with this Act;

(b) the Controller in framing the regulations under this Act.

(4) There shall be paid to the non-official members of such Committee such travelling and other allowances as the Government may fix.

(5) The term of office of the Chairman and the members of the Cyber Regulations Advisory Committee may be fixed by the Government."

As a result of enactment of the proposed Act, certain consequential amendments are required to be made in the Penal Code, 1860, the Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Bangladesh Bank Order, 1972. The proposed amendments are as follows:-

"98. Amendments of other Acts.- (1) The Penal Code, 1860 (Act XLV of 1860) shall be amended in the manner specified in the First Schedule to this Act.

(2) The Evidence Act, 1872 (Act I of 1872) shall be amended in the manner specified in the Second Schedule to this Act.

(3) The Bankers' Books Evidence Act, 1891 (Act XVIII of 1891) shall be amended in the manner specified in the Third Schedule to this Act.

(4) The Bangladesh Bank Order, 1972 (President's Order No. 127 of 1972) shall be amended in the manner specified in the Fourth Schedule to this Act.

The First Schedule

(See section 97 (1)

Amendments to the Penal Code, 1860 (Act XLV of 1860).

1. After section 29, the following section shall be inserted, namely:-

"29 A. Electronic record.- The words, "electronic record", shall have the meaning assigned to them in clause (t) of section 3 of the Information Technology (Electronic Transaction) Act, 20....."

2. In section 167, for the words, "such public servant, charged with the preparation or translation of any document, frames or translates that document," the words, "such public servant, charged with the preparation or translation of any document or electronic record, frames, prepares or translates that document or electronic record," shall be substituted.

3. In section 172, for the words, "produce a document in a Court of Justice," the words, "produce a document or electronic record in a Court of Justice," shall be substituted.

4. In section173, for the words, "to produce a document in a Court of Justice ," the words, "to produce a document or electronic record in a Court of Justice," shall be substituted.

5. In section 175, for the word, "document", at both the places where it occurs, the words, "document or electronic record," shall be substituted.

6. In section 192, for the words, "makes any false entry in any book or record, or makes any document containing a false statement," the words, "makes any false entry in any book or record or electronic record or makes any document or electronic record containing a false statement," shall be substituted.

7. In section 204, for the word, “document,” at both the places where it occurs, the words, “document or electronic record,” shall be substituted.

8. In section 463, for the words, “Whoever makes any false documents or part of a document with intent to cause damage or injury,” the words, “Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury,” shall be substituted.

9. In section 464,

(a) for the portion beginning with the words, “A person is said to make a false document,” and ending with the words, “by reason of deception practised upon him, he does not know the contents of the document or the nature of the alteration,” the following shall be substituted, namely:-

“A person is said to make a false document or false electronic record -

First- Who dishonestly or fraudulently-

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any digital signature on any electronic record;

(d) makes any mark denoting the execution of a document or the authenticity of the digital signature,

with the intention of causing it to be believed that such document or part of document, electronic record or digital signature was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, signed, sealed, executed or affixed; or

Secondly- Who, without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with digital

signature either by himself or by any other person, whether such person be living or dead at the time of such alteration; or

Thirdly- Who dishonestly or fraudulently causes any person to sign, seal, execute or alter a document or an electronic record or to affix his digital signature on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document or electronic record or the nature of the alteration.",

(b) after Explanation 2, the following Explanation shall be inserted at the end, namely:-

"Explanation 3- For the purposes of this section, the expression, "affixing digital signature", shall have the meaning assigned to it in clause (e) of section 3 of the Information Technology (Electronic Transaction) Act, 20....."

10. In section 466.-

(a) for the words, "Whoever forges a document," the words, "Whoever forges a document or an electronic record," shall be substituted;

(b) the following Explanation shall be inserted at the end, namely:-

"Explanation.- For the purposes of this section, "register" includes any list, data or record of any entries maintained in the electronic form as defined in clause (r) of section 3 of the Information Technology (Electronic Transaction) Act, 20....."

11. In section 468, for the words, "document forged", the words, "document or electronic record forged", shall be substituted.

12. In section 469, for the words, "intending that the document forged," the words, "intending that the document or electronic record forged," shall be substituted.

13. In section 470, for the word, “document”, in both the places where it occurs, the words, “document or electronic record,” shall be substituted.

14. In section 471, for the word, “document,” whe rever it occurs, the words, “document or electronic record”, shall be substituted.

15. In section 474, for the portion beginning with the words, “Whoever has in his possession any document,” and ending with the words, “if the document is one of the description mentioned in section 466 of this Code,” the following shall be substituted, namely:-

“Whoever has in his possession any document or electronic record, knowing the same to be forged and intending that the same shall fraudulently or dishonestly be used as genuine, shall, if the document or electronic record is one of the description mentioned in section 466 of this Code,”

16. In section 476, for the words, “any document,” the words, “any document or electronic record,” shall be substituted.

17. In section 477 A, for the words, “book, paper, writing,” at both the places where they occur, the words, “book, electronic record, paper, writing”, shall be substituted.

The Second Schedule
(Sec section 97 (2))
Amendments to the Evidence Act, 1872 (Act I of 1872)

1. In section 3,-

(a) in the definition of “Evidence”, for the words, “all documents produced for the inspection of the Court,” the words, “all documents including electronic records produced for the inspection of the Court,” shall be substituted;

(b) after the definition of “not proved”, the following shall be inserted, namely:-

"the expressions, "addressee", "Certifying Authority", "Controller", "digital signature", "Digital Signature Certificate," "electronic form", "electronic record," "information," "originator", secure electronic record," "secure digital signature" and "subscriber" shall have the meaning respectively assigned to them in the Information Technology (Electronic Transaction) Act, 20....."

2. In section 17, for the words, "oral or documentary", the words, "oral or documentary or contained in electronic form," shall be substituted.

3. After section 22, the following section shall be inserted, namely:-

"22A. When oral admission as to contents of electronic records are relevant.- Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question."

4. In section 34, for the words, "Entries in the books of account," the words, "Entries in the books of accounts, including those maintained in an electronic form," shall be substituted.

5. In section 35, for the word, "record", in both the places where it occurs, the words, "record or an electronic record," shall be substituted.

6. For section 39, the following section shall be substituted, namely:-

"39. What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.-When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of an electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers

necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made."

7. After section 47, the following section shall be inserted, namely:-

"47 A. Opinion as to digital signature when relevant.- When the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact."

8. In section 59, for the words, "contents of documents," the words, "contents of documents or electronic records," shall be substituted.

9. After section 65, the following section shall be inserted, namely:-

"65 A. Special provisions as to evidence relating to electronic records.- The contents of electronic records may be proved in accordance with the provisions of section 65 B.

65 B. Admissibility of electronic records.- (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section, (1) of this section in respect of a computer output shall be the following, namely:-

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities

regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the period referred to in clause (a) of this sub-section, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the period referred to in clause (a) of this sub-section, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) of this section was regularly performed by computers, whether-

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers,

all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say-

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) of this section relate,

and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,-

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any officials, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that

computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation.- For the purposes of this section, any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process."

10. After section 67, the following section shall be inserted, namely:-

"67 A. Proof as to digital signature.- Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record, the fact that such digital signature is the digital signature of that subscriber must be proved."

11. After section 73, the following section shall be inserted, namely:-

"73 A. Proof as to verification of digital signature.- In order to ascertain whether a digital signature is that of the person, by whom it purports to have been affixed, the Court may direct-

(a) that person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;

(b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person."

12. After section 84, the following section shall be inserted, namely:-

"84A. Presumption as to Gazettes in electronic forms.- The Court shall presume the genuineness of every electronic record purporting to be the Official Gazette, or purporting to be electronic record directed by any law to be

kept by any person, if such electronic record is kept substantially in the form required by law and is produced from proper custody."

13. After section 85, the following sections shall be inserted, namely:-

"85A. Presumption as to electronic agreements.- The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signatures of the parties."

85B. Presumption as to electronic records and digital signatures.- (1) In any proceedings involving a secure electronic record, the Court shall presume, unless the contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings involving secure digital signature, the Court shall presume, unless the contrary is proved, that

(a) the secure digital signature is affixed by the subscriber with the intention of signing or approving the electronic record;

(b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to the authenticity and integrity of the electronic record or any digital signature.

85C. Presumption as to Digital Signature Certificates.- The Court shall presume, unless the contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber."

14. After section 88, the following section shall be inserted, namely:-

"88A. Presumption as to electronic messages.- The Court may presume that an electronic message forwarded by the originator through an

electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent."

15. After section 90, the following section shall be inserted, namely:-

"90A. Presumption as to electronic records five years old.- Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by that person or any person authorised by him in this behalf.

Explanation.- Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they would naturally be; but no custody is improper if it is proved to have had a legitimate origin, or if the circumstances of the particular case are such as to render such an origin probable.

This Explanation applies also to section 84A."

16.For section 131, the following section shall be substituted, namely:-

"131. Production of documents or electronic records which another person, having possession, could refuse to produce.- No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production."

The Third Schedule

(See section 97 (3)

Amendments to the Bankers' Books Evidence Act, 1891,

(Act XVIII of 1891)

1. In section 2,-

(a) for clause (3), the following clause shall be substituted, namely:-

"(3) "bankers' books" include ledgers, day-books, cash-books, account books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device;"

(b) for clause (8), the following clause shall be substituted, namely:-

"(8) "certified copy" means when the books of a bank,-

(a) are maintained in written form, a copy of any entry in such books together with a certificate written at the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and

(b) consist of printout of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A."

2. After section 2, the following section shall be inserted, namely:-

"2A. Conditions in the printout.- A printout of an entry or a copy of a printout referred to in clause (8) of section 2 of this Act shall be accompanied by the following, namely:-

(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and

(b) a certificate by a person in-charge of the computer system containing a brief description of the computer system and the particulars of-

(i) the safeguards adopted by the system to ensure that data is entered or any other operation is performed only by authorised persons;

(ii) the safeguards adopted to prevent and detect unauthorised change of data;

(iii) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(iv) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;

(v) the mode of verification in order to ensure that data has been accurately transferred to such removable media;

(vi) the mode of identification of such data storage devices;

(vii) the arrangements for the storage and custody of such storage devices;

(viii) the safeguards to prevent and detect any tampering with the system; and

(ix) any other factor which will vouch for the integrity and accuracy of the system.

(c) a further certificate from the person in-charge of the computer system to the effect that to the best of his knowledge and belief, such computer system operated properly at the material time, he was provided with all the relevant data and the printout in question represents correctly, or is appropriately derived from, the relevant data."

The Fourth Schedule
(See section 97 (4)
Amendment to the Bangladesh Bank Order, 1972
(President's Order No. 127 of 1972)

In the Bangladesh Bank Order, 1972, in article 82, in clause (2) after sub-clause (k), the following sub-clause shall be inserted, namely:-

"(kk) the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions referred to in clause (c) of article 50, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers."

Justice A.K.M. Sadeque
Member
Law Commission

Justice Naimuddin Ahmed
Member
Law Commission

Justice A.T.M. Afzal
Chairman
Law Commission